UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/608,653	06/27/2003	Dinarte R. Morais	MS1-1430US	7042

22801 7590 10/26/2006

LEE & HAYES PLLC
421 W RIVERSIDE AVENUE SUITE 500
SPOKANE, WA 99201

EXAMINER	
LOVING, JARIC E	

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 10/26/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/608,653	MORAIS ET AL.	
	Examiner	Art Unit	
	Jaric Loving	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *27 June 2003*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-59* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-59* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *27 June 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *11/24/03, 1/25/05*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Specification

1. The disclosure is objected to because of the following informalities: on page 22, paragraph [0071], a set of parenthesis are missing an opening and closing, respectively.

Appropriate correction is required.

Claim Objections

2. Claim 8 is objected to because of the following informalities: line 7 recites "an denial". It should be --a denial--. Appropriate correction is required.

3. The numbering of claims is not in accordance with 37 CFR 1.126 which requires the original numbering of the claims to be preserved throughout the prosecution. When claims are canceled, the remaining claims must not be renumbered. When new claims are presented, they must be numbered consecutively beginning with the number next following the highest numbered claims previously presented (whether entered or not).

There are two claim 36's. Claims 37-44, depend on claim 36, but it is unclear to which 36. The second 36 will be treated as the parent claim for the remainder of this office action.

Claim Rejections - 35 USC § 101

4. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 29-36 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. On page 8, paragraph [0023], applicant provides, "... computer readable media may comprise... communication media." On

page 9, paragraph [0024], applicant further states, "Communication media typically embodies computer readable instructions... or other data in a modulated data signal such as a carrier wave or other transport mechanism..."

Therefore, the claims lack the necessary physical articles or objects to constitute a machine or a manufacture within the meaning of §101. They are clearly not a series or steps or acts to be a process nor are they a combination of chemical compounds to be a composition of matter. As such, they fail to fall within a statutory category. They are, at best, functional descriptive material *per se*.

Claim Rejections - 35 USC § 102

5. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

6. Claims 1-15, 29-36, and 45-49 are rejected under 35 U.S.C. 102(e) as being anticipated by Newcombe, US 2003/0172269.

In claim 1, Newcombe discloses a process for requesting authentication comprising:

transmitting data from a hash digest formed using client-specific data together with second client specific data (paragraphs [0025], [0056]-[0059], [0065]-[0067]); and

receiving, in response to transmitting, an indication of acceptance when the data from the hash digest corresponds to a valid client authentication request (paragraphs [0042], [0059], [0061]-[0062]).

In claim 2, Newcombe discloses the process of claim 1, further comprising, prior to transmitting, computing the hash digest using first client specific data comprising a valid client name together with a time-varying function (paragraphs [0025], [0057]-[0058], [0066]-[0067]).

In claim 3, Newcombe discloses the process of claim 1, further comprising, prior to transmitting, computing a hash digest using an HMAC algorithm and wherein the data from the hash digest include a truncated hash digest (paragraphs [0030], [0103], [0107]).

In claim 4, Newcombe discloses the process of claim 1, further comprising, prior to transmitting, computing a hash digest using the client name, client key and a function of time, and wherein transmitting includes transmitting a current time (paragraphs [0025], [0029]-[0032], [0056]-[0059], [0065]-[0067]).

In claim 5, Newcombe discloses the process of claim 1, further comprising, prior to transmitting, computing a hash digest using first client-specific data comprising a valid client name together with a key corresponding to the valid client name, and a current time (paragraphs [0025], [0029]-[0032], [0056]-[0059], [0065]-[0067]).

In claim 6, Newcombe discloses the process of claim 1, wherein transmitting comprises transmitting the hash digest together with a valid client name corresponding to the hash digest (paragraphs [0025], [0065]-[0067]).

In claim 7, Newcombe discloses the process of claim 1, further comprising, prior to transmitting, computing a hash digest using first client-specific data comprising a valid client name together with a key corresponding to the valid client name; and wherein transmitting comprises transmitting the hash digest together with a valid client name corresponding to the hash digest (paragraphs [0025], [0056]-[0059], [0065]-[0067]).

In claim 8, Newcombe discloses a process for requesting authentication comprising:

transmitting a hash digest formed from first client-specific data together with second client specific data (paragraphs [0025], [0056]-[0059], [0065]-[0067]);

receiving, in response to transmitting, an indication of acceptance when the hash digest and second client-specific data correspond to a valid client authentication request (paragraphs [0042], [0059], [0061]-[0062]); and

receiving, in response to transmitting, an denial of authentication when the hash digest or the second client-specific data do not correspond to a valid client authentication request (paragraphs [0042], [0059], [0061]-[0062]).

In claim 9, Newcombe discloses the process of claim 8, further comprising, prior to transmitting, computing the hash digest from first client-specific data and a time-varying function (paragraphs [0025], [0057]-[0058], [0066]-[0067]).

In claim 10, Newcombe discloses the process of claim 8, wherein transmitting a hash digest includes transmitting a hash digest computed using first client specific data

comprising a valid client name together with a client key (paragraphs [0025], [0029]-[0032], [0056]-[0059], [0065]-[0067]).

In claim 11, Newcombe discloses the process of claim 8, wherein transmitting a hash digest comprises transmitting a hash digest formed using an HMAC algorithm (paragraphs [0030], [0103], [0107]).

In claim 12, Newcombe discloses the process of claim 8, wherein transmitting a hash digest comprises transmitting a hash digest computed using first client-specific data comprising a valid client name together with a key corresponding to the valid client name and a current time (paragraphs [0025], [0029]-[0032], [0056]-[0059], [0065]-[0067]).

In claim 13, Newcombe discloses the process of claim 8, wherein transmitting a hash digest comprises transmitting a hash digest computed using first client-specific data comprising a valid client name together with a key corresponding to the valid client name, and a current time, and wherein transmitting includes transmitting the current time (paragraphs [0025], [0029]-[0032], [0056]-[0059], [0065]-[0067]).

In claim 14, Newcombe discloses the process of claim 8, wherein transmitting comprises transmitting the hash digest together with a valid client name corresponding to the hash digest (paragraphs [0025], [0065]-[0067]).

In claim 15, Newcombe discloses the process of claim 8, wherein transmitting a hash digest comprises transmitting a valid client name together with a hash digest computed using and HMAC algorithm and first client-specific data comprising a valid

client name together with a key corresponding to the valid client name, and a current time (paragraphs [0025], [0029]-[0032], [0056]-[0059], [0065]-[0067], [0103], [0107]).

In claim 29, Newcombe discloses one or more computer-readable media including instructions that, when executed by one or more processors, causes the one or more processors to:

form an encrypted data string including first client-specific information (paragraphs [0056]-[0059], [0065]);

transmit a message including credentials formed using the encrypted data string together with second client-specific information (paragraph [0025]); and

receive an authentication for system access, in response to the message, when the credentials are valid (paragraphs [0042], [0059], [0061]-[0062]).

In claim 30, Newcombe discloses the computer-readable media of claim 29, wherein the code configured to cause the one or more processors to form an encrypted data string comprises code configured to cause the one or more processors to form a hash digest from a function of time and a client key (paragraphs [0056]-[0059], [0065]).

In claim 31, Newcombe discloses the computer-readable media of claim 29, wherein the code configured to cause the one or more processors to form an encrypted data string comprises code configured to cause the one or more processors to form an encrypted data string from one or more of: a name, a NameHash, a truncation of a NameHash, a NameKeyHash, a truncation of a NameKeyHash, a TimedNameKeyHash, a truncation of a TimedNameKeyHash or a time (paragraphs [0025], [0056]-[0059], [0065]-[0067]).

In claim 32, Newcombe discloses the computer-readable media of claim 29, wherein the code configured to cause the one or more processors to form an encrypted data string comprises code configured to cause the one or more processors to form an encrypted data string using a one-way hash function (paragraphs [0029]-[0030], [0056]-[0059], [0065]).

In claim 33, Newcombe discloses the computer-readable media of claim 29, wherein the code configured to cause the one or more processors to form an encrypted data string comprises code configured to cause the one or more processors to form a hash digest using an HMAC algorithm (paragraphs [0030], [0056]-[0059], [0065]).

In claim 34, Newcombe discloses the computer-readable media of claim 29, wherein the code configured to cause the one or more processors to form an encrypted data string comprises code configured to cause the one or more processors to form an encrypted data string using a valid client name and a current time together with a key corresponding to the valid client name (paragraphs [0025], [0029]-[0032], [0056]-[0059], [0065]-[0067]).

In claim 35, Newcombe discloses the computer-readable media of claim 29, wherein the code configured to cause the one or more processors to form an encrypted data string comprises code configured to cause the one or more processors to form an encrypted data string using a key corresponding to the valid client name and a current time (paragraphs [0025], [0029]-[0032], [0056]-[0059], [0065]-[0067]).

In claim 36, Newcombe discloses the computer-readable media of claim 29, wherein the code configured to cause the one or more processors to transmit comprises

code that is configured to cause the one or more processors to transmit a plaintext client name as a portion of the second client-specific data (paragraphs [0025], [0056]-[0059], [0065]-[0067]).

In claim 45, Newcombe discloses an authentication process comprising:

transmitting, by a user, client specific data including at least one of first client specific data, a client name and a proof of knowledge of a client key (paragraphs [0025], [0056]-[0059], [0065]-[0067]); and

receiving, in response to transmitting, an authentication to access a remote computer (paragraphs [0042], [0059], [0061]-[0062]).

In claim 46, Newcombe discloses the authentication process comprising:

transmitting, by a user, client specific data including at least one of first client specific data, a client name, proof of knowledge of a client key and a NameKeyHash (paragraphs [0025], [0056]-[0059], [0065]-[0067]); and

receiving, in response to transmitting, an authentication to access a remote computer (paragraphs [0042], [0059], [0061]-[0062]).

In claim 47, Newcombe discloses the process of claim 46, wherein transmitting includes transmitting a truncation of the NameKeyHash formed using the client key and client name (paragraphs [0065]-[0067], [0103], [0107]).

In claim 48, Newcombe discloses an authentication process comprising:

transmitting, by a user, client specific data including at least one of first client specific data, a client name, a TimedNameKeyHash and a current time (paragraphs [0025], [0056]-[0059], [0065]-[0067]); and

receiving, in response to transmitting, an authentication to access a remote computer (paragraphs [0042], [0059], [0061]-[0062]).

In claim 49, Newcombe discloses the process of claim 48, wherein the TimedNameKeyHash is formed using the current time, the client name and the client key (paragraphs [0025], [0056]-[0059], [0065]-[0067]).

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. Claims 16-28, 36-44, and 50-59 are rejected under 35 U.S.C. 103(a) as being unpatentable over Newcombe and further in view of Chang et al., US 6,952,781.

In claim 16, Newcombe discloses a process for verification of a client authentication request by a server, comprising:

receiving, in the server, a client authentication request including client specific data (paragraphs [0025], [0056]-[0057], [0067]);

comparing the client specific data to data stored in a server coupled to the server to determine that the client specific data meet a first threshold of validity (paragraphs [0063]-[0064] – one or more content servers).

Newcombe fails to disclose a cache memory; when comparing determines that the client specific data meet the first threshold of validity, proceeding with the authentication process; and when comparing determines that the client specific data do

not meet the first threshold of validity, terminating the verification process. Chang discloses a cache memory (col. 4, lines 17-24; col. 6, lines 2-3); when comparing determines that the client specific data meet the first threshold of validity, proceeding with the authentication process (col. 4, lines 25-39 – client data must pass AAA server before proceeding to network access server); and when comparing determines that the client specific data do not meet the first threshold of validity, terminating the verification process (col. 6, lines 47-50).

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine Newcombe's method of authentication with Chang's security server system utilizing a cache memory and a first threshold of validity to enhance data manipulation. It is for this reason that one of ordinary skill in the art would have been motivated to provide Newcombe's method of authentication with a cache memory and a first threshold of validity because it streamlines user validation without requiring the user to enter identification a second time (Chang, col. 2, lines 55-63; col. 3, lines 8-19).

In claim 17, Newcombe, as modified, discloses process of claim 16, further comprising, when comparing determines that the client specific data do not meet the first threshold, storing a portion of the client specific data in a second cache memory along with an indication that the client specific data do not correspond to a valid client (Newcombe, paragraphs [0063]-[0064]; Chang, col. 4, lines 17-24; col. 6, lines 2-3 and lines 47-50).

In claim 18, Newcombe, as modified, discloses the process of claim 16, wherein:

proceeding with the authentication process comprises second comparing the client specific data with data stored in a second cache memory to determine when the client specific data meet a second threshold of validity and when the client specific data correspond to an identity previously determined to be valid or invalid (Newcombe, paragraphs [0025], [0063]-[0064]; Chang, col. 4, lines 17-24; col. 6, lines 2-3 and lines 47-50); and

when the client specific data meet the second threshold, transmitting a request for verification to a database containing client-specific data (Newcombe, paragraphs [0042], [0059], [0061]-[0062]); and

when the client specific data correspond to an identity previously determined to be invalid, terminating the authentication request (Chang, col. 6, lines 47-50).

In claim 19, Newcombe, as modified, discloses the process of claim 16, wherein receiving comprises receiving data including one or more of: a name, a NameHash, a truncation of a NameHash, a NameKeyHash, a truncation of a NameKeyHash, a TimedNameKeyHash, a truncation of a TimedNameKeyHash or a time (Newcombe, paragraphs [0025], [0056]-[0059], [0065]-[0067]).

In claim 20, Newcombe, as modified, discloses the process of claim 16, wherein receiving comprises receiving a TimedNameKeyHash (Newcombe, paragraphs [0025], [0056]-[0059], [0065]-[0067]).

In claim 21, Newcome, as modified, discloses the process of claim 16, wherein receiving comprises receiving a TimedNameKeyHash and a current time (Newcombe, paragraphs [0025], [0056]-[0059], [0065]-[0067]).

In claim 22, Newcombe, as modified, discloses the process of claim 16, wherein comparing the client specific data to data stored in a first cache memory comprises comparing a TimedNameKeyHash contained in the authentication request to a function of a stored NameKeyHash and a current time (Newcombe, paragraphs [0042], [0059], [0061]-[0062]; Chang, col. 4, lines 17-24; col. 6, lines 2-3).

In claim 23, Newcombe, as modified, discloses the process of claim 16, wherein receiving client specific data includes receiving a current time, and further comprising determining when the received current time disagrees with another current time used by the authentication server, and, when the received current time and the another current time disagree, sending the another current time to an originator of the authentication request (Chang, col. 7, line 58 – col. 8, line 2).

In claim 24, Newcombe discloses a process for updating a cache memory associated with an authentication server comprising:

sending a request to a database containing information describing authentic users, the request requesting information associated with authentic users that have been entered in the database after a predetermined time (paragraphs [0060]-[0063]);

receiving data corresponding to authentic users where the data have been entered to the database after the predetermined time (paragraphs [0059]-[0063]).

Newcombe fails to disclose storing at least a portion of the received data in the cache memory. Chang discloses storing at least a portion of the received data in the cache memory (col. 4, lines 17-24; col. 6, lines 2-3).

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine Newcombe's method of authentication with Chang's security server system utilizing a cache memory to enhance data manipulation. It is for this reason that one of ordinary skill in the art would have been motivated to provide Newcombe's method of authentication with a cache memory because it streamlines user validation without requiring the user to enter identification a second time (Chang, col. 2, lines 55-63; col. 3, lines 8-19).

In claim 25, Newcombe, as modified, discloses the process of claim 24, wherein sending a request comprises sending a request for information associated with authentic users that have been added to the database since a previous such request was made (Newcombe, paragraphs [0059]-[0063]).

In claim 26, Newcombe, as modified, discloses the process of claim 24, wherein receiving comprises receiving a name and a key and the name, and further comprising:

forming a hash digest using the name and a random session key (Newcombe, paragraphs [0065]-[0066]); and

storing client-specific data in the cache memory such that the hash digest may be used as a cachekey to access the client-specific data (Newcombe, paragraphs [0063], [0065]-[0067]; Chang, col. 4, lines 17-24; col. 6, lines 2-3).

In claim 27, Newcombe, as modified, discloses the process of claim 24, further comprising computing a hash digest from a valid user name contained in the received data and a random session key stored in the authentication server (Newcombe, paragraphs [0065]-[0066]).

In claim 28, Newcombe, as modified, discloses the process of claim 24, further comprising:

computing a hash digest from one or more of a valid user name, an associated key and a random session key (Newcombe, paragraphs [0065]-[0066]),

truncating the hash digest (Newcombe, paragraph [0103], [0107]); and

storing client-specific data in the cache memory such that the truncated hash digest may be used as a cachekey to access the client-specific data (Newcombe, paragraphs [0061]-[0063], [0065]-[0067]; Chang, col. 4, lines 17-24; col. 6, lines 2-3).

In claim 36, Newcombe discloses a computer system comprising:

an authentication server (paragraph [0054]); and

a server coupled to the authentication server, wherein the authentication server is configured to (paragraphs [0037], [0054], [0063]-[0064]):

receive a client authentication request including client-specific data (paragraph [0025]).

Newcombe fails to disclose a primary cache memory; comparing the client specific data to data stored in a first cache memory coupled to the server to determine that the client specific data meet a first threshold of validity; when comparing determines that the client specific data meet the first threshold of validity, proceed with authentication; and when comparing determines that the client specific data do not meet the first threshold of validity, terminate authentication and deny authentication request. Chang discloses a primary cache memory (col. 4, lines 17-24; col. 6, lines 2-3); comparing the client specific data to data stored in a first cache memory coupled to the

server to determine that the client specific data meet a first threshold of validity (col. 4, lines 25-39); when comparing determines that the client specific data meet the first threshold of validity, proceed with authentication (col. 4, lines 25-39); and when comparing determines that the client specific data do not meet the first threshold of validity, terminate authentication and deny authentication request (col. 6, lines 47-50).

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine Newcombe's method of authentication with Chang's security server system utilizing a cache memory and a first threshold of validity to enhance data manipulation. It is for this reason that one of ordinary skill in the art would have been motivated to provide Newcombe's method of authentication with a cache memory and a first threshold of validity because it streamlines user validation without requiring the user to enter identification a second time (Chang, col. 2, lines 55-63; col. 3, lines 8-19).

In claim 37, Newcombe, as modified, discloses the computer system of claim 36, wherein the authentication server is configured to employ a first, plaintext portion of the client-specific data as a cachekey to obtain related encrypted client-specific data from the first cache memory (Newcombe, paragraphs [0025], [0056]-[0059], [0063], [0065]-[0067]; Chang, col. 4, lines 17-24; col. 6, lines 2-3).

In claim 38, Newcombe, as modified, discloses the computer system of claim 36, wherein the authentication server is further configured to store at least some of the client specific data in a second cache memory along with an indication that the client specific data do not correspond to a valid client when comparing determines that the

client specific data do not meet the first threshold (Newcombe, paragraphs [0025], [0042], [0047]-[0048]; Chang, col. 4, lines 17-24; col. 6, lines 2-3 and lines 47-50).

In claim 39, Newcombe, as modified, discloses the computer system of claim 36, wherein the authentication server is configured to second compare the client specific data with data stored in a second cache memory to determine when the client specific data meet a second threshold of validity and when the client specific data correspond to an identity previously determined to be valid or invalid (Newcombe, paragraphs [0025], [0042], [0047]-[0048]; Chang, col. 4, lines 17-24; col. 6, lines 2-3 and lines 47-50).;

when the client specific data meet the second threshold, transmit a request for verification to a database containing client-specific data (Newcombe, paragraphs [0054]-[0057], [0068]-[0069]); and

when the client specific data correspond to an identity previously determined to be invalid, terminate the authentication request (Newcombe, paragraph [0063]).

In claim 40, Newcombe, as modified, discloses the computer system of claim 36, wherein the client-specific data includes a NameKeyHash that is also a function of time (Newcombe, paragraphs [0025], [0056]-[0059], [0065]-[0067]).

In claim 41, Newcombe, as modified, discloses the computer system of claim 36, wherein the client-specific data includes a TimedNameKeyHash (Newcombe, paragraphs [0025], [0056]-[0059], [0065]-[0067]).

In claim 42, Newcombe, as modified, discloses the computer system of claim 36, wherein the client-specific data includes a TimedNameKeyHash and a current time is

included with the clientspecific data (Newcombe, paragraphs [0025], [0056]-[0059], [0065]-[0067]).

In claim 43, Newcombe, as modified, discloses the computer system of claim 36, wherein the client specific data stored in the first cache memory comprises a NameKeyHash, and wherein the authentication server is configured to form a TimedNameKeyHash from the NameKeyHash and to compare the formed TimedNameKeyHash to a portion of the client-specific data (Newcombe, paragraphs [0025], [0056]-[0059], [0063]-[0067]; Chang, col. 4, lines 17-24; col. 6, lines 2-3).

In claim 44, Newcombe, as modified, discloses the computer system of claim 36, wherein the client specific data includes a current time, and wherein the authentication server is further configured to determine when the received current time disagrees with another current time used by the authentication server, and when the received current time and the another current time disagree, send the another current time to an originator of the authentication request (Chang, col. 7, line 58 – col. 8, line 2).

In claim 50, Newcombe discloses a process for authenticating a user, comprising:

receiving an authentication request including first client specific data comprising at least one of a client name and proof of knowledge of a client key (paragraphs [0025], [0056]-[0059], [0065]-[0067]);

computing a NameHash using the received client name and a random session key (paragraphs [0065]-[0066]);

using data corresponding to the NameHash as a key to access data from a server (paragraphs [0063]-[0067]).

Newcombe fails to disclose a cache; a first validity threshold; comparing the first validity threshold data to the first client specific data; and terminating authentication when the first validity threshold data do not match the first client data. Chang discloses a cache (col. 4, lines 17-24; col. 6, lines 2-3); a first validity threshold (col. 4, lines 25-39); comparing the first validity threshold data to the first client specific data (col. 4, lines 25-39); and terminating authentication when the first validity threshold data do not match the first client data (col. 6, lines 47-50).

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine Newcombe's method of authentication with Chang's security server system utilizing a cache and a first threshold of validity to enhance data manipulation. It is for this reason that one of ordinary skill in the art would have been motivated to provide Newcombe's method of authentication with a cache and a first threshold of validity because it streamlines user validation without requiring the user to enter identification a second time (Chang, col. 2, lines 55-63; col. 3, lines 8-19).

In claim 51, Newcombe, as modified, discloses the process of claim 50, further comprising, when the first validity data do not match the first client data, storing the client key and a CredentialInvalidFlag in a second cache memory (Newcombe, paragraphs [0063]-[0065]; Chang, col. 4, lines 17-24; col. 6, lines 2-3).

In claim 52, Newcombe, as modified, discloses the process of claim 50, further comprising, when the first validity data do match the first client data, employing the

client name as a cachekey to access second client validity data from a second cache memory (Newcombe, paragraphs [0063]-[0065]; Chang, col. 4, lines 17-24; col. 6, lines 2-3).

In claim 53, Newcombe, as modified, discloses the process of claim 50, further comprising, when the first validity data do match the first client data, employing the client name as a cachekey to access second client validity data from a second cache memory, wherein the second client validity data comprise a stored copy of a client key (Newcombe, paragraphs [0063]-[0065]; Chang, col. 4, lines 17-24; col. 6, lines 2-3).

In claim 54, Newcombe, as modified, discloses the process of claim 50, wherein using data corresponding to the NameHash as a cachekey comprises using a truncation of the NameHash to access first validity threshold data from a first cache memory (Newcombe, paragraphs [0063], [0065]-[0067], [0103], [0107]; Chang, col. 4, lines 17-39; col. 6, lines 2-3).

In claim 55, Newcombe discloses a process for authenticating a user, comprising:

receiving an authentication request including at least one of first client specific data comprising at least one of a client name, proof of knowledge of a client key and a NameKeyHash (paragraphs [0042], [0059], [0061]-[0062]).

computing a NameHash using the received client name and a random session key (paragraphs [0065]-[0066]);

using data corresponding to the NameHash as a key (paragraphs [0025], [0056]-[0059], [0065]-[0067]).

Newcombe fails to disclose a cache; access first validity threshold data from a first cache memory; comparing the first validity threshold data to the first client data; and terminating authentication when the first validity threshold data do not match the first client data. Chang discloses a cache (col. 4, lines 17-24; col. 6, lines 2-3); access first validity threshold data from a first cache memory (col. 4, lines 17-39; col. 6, lines 2-3); comparing the first validity threshold data to the first client data (col. 4, lines 25-39); and terminating authentication when the first validity threshold data do not match the first client data (col. 6, lines 47-50).

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine Newcombe's method of authentication with Chang's security server system utilizing a cache and a first threshold of validity to enhance data manipulation. It is for this reason that one of ordinary skill in the art would have been motivated to provide Newcombe's method of authentication with a cache and a first threshold of validity because it streamlines user validation without requiring the user to enter identification a second time (Chang, col. 2, lines 55-63; col. 3, lines 8-19).

In claim 56, Newcombe, as modified, discloses the process of claim 55, further comprising, when the first validity data do not match the first client data, storing the client key and a CredentialInvalidFlag in a second cache memory (Newcombe, paragraphs [0063]-[0065]; Chang, col. 4, lines 17-24; col. 6, lines 2-3).

In claim 57, Newcombe, as modified, discloses the process of claim 55, further comprising, when the first validity data do match the first client data, employing the client name as a cachekey to access second client validity data from a second cache

memory (Newcombe, paragraphs [0063]-[0065]; Chang, col. 4, lines 17-24; col. 6, lines 2-3).

In claim 58, Newcombe, as modified, discloses the process of claim 55, further comprising, when the first validity data do match the first client data, employing the client name as a cachekey to access second client validity data from a second cache memory, wherein the second client validity data comprise a stored copy of a client key (Newcombe, paragraphs [0063]-[0065]; Chang, col. 4, lines 17-24; col. 6, lines 2-3).

In claim 59, Newcombe, as modified, discloses the process of claim 55, wherein using data corresponding to the NameHash as a cachekey comprises using a truncation of the NameHash to access first validity threshold data from a first cache memory (Newcombe, paragraphs [0063], [0065]-[0067], [0103], [0107]; Chang, col. 4, lines 17-39; col. 6, lines 2-3).

Conclusion

9. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure: Sandhu et al., US 7,069,435; Carman et al., US 6,272,632; Wright, US 5,633,931; Haynes, III et al., US 6,161,181; Stamos et al., US 7,100,047; Newcombe et al., US 2003/0172270; Subramaniam et al., US 2004/0049702; Buer, US 2004/0247131.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jaric Loving whose telephone number is (571) 272-1686. The examiner can normally be reached on Monday-Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

JL

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER